Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A web-based method for applying a legally enforceable signature of a user on an electronic document located on a server, the signing of said document occurring in a web environment, said method comprising the steps of:

a) having the user access the web environment through a web browser from a secure electronic system, said secure system having verified the identity of the user;

b) having the user sign the electronic document in said web environment, said signing ~~being server-based and~~ comprising modules on the server performing the substeps of:

i) presenting the user with a web-based representation of the document in said web browser;

ii) presenting the user with legal information related to said signing, and getting agreement from the user of said legal information in said web browser; and

iii) upon agreement ~~from the user~~ of the legal information from the user, applying said signature of the user on said document on the server;

c) on the server, generating a process log of the signing of step b), said process log comprising a record ~~allowing the reconstruction~~ of substeps b) i) to b) iii) as executed ~~by said user~~ and allowing the reconstruction of the web-based representation of the document and of the legal information as presented to the user through said web browser, and securely associating said process log with the document as signed, said securely associating comprising the substeps of:

i) generating a secure process authentication code uniquely representing said process log, said secure process authentication code being a hash of said process log; and

ii) embedding said process authentication code in said document as signed, thereby securely associating said process log and document; and

d) making the document as signed available to the user.

2. (Original) A method according to claim 1, wherein substep b) i) comprises retrieving said document from a document storing location.

3. (Original) A method according to claim 1, wherein substep b) i) comprises generating said document from a template.

4. (Original) A method according to claim 1, wherein substep b) i) comprises transforming said document from a non-web format to a web-format.

5. (Original) A method according to claim 1, wherein, in step b) ii), said legal information comprises information about legal implications of the signing of the document.

6. (Original) A method according to claim 1, wherein, in step b) ii), said legal information comprises legal disclosures related to said document.

7. (Original) A method according to claim 1, wherein substep b) ii) comprises presenting said legal information in a series of web pages.

8. (Original) A method according to claim 1, wherein substep b) ii) comprises presenting said legal information in a series of dialog boxes.

9. (Original) A method according to claim 1, wherein substep b) iii) comprises associating user-specific information to said document.

10. (Original) A method according to claim 9, wherein, in substep b) iii), said user-specific information is included in a special signature file defining the signature of the user.

11. (Original) A method according to claim 9, wherein substep b) iii) further comprises associating a digital certificate and private key to the document.

12. (Original) A method according to claim 9, wherein substep b) iii) further comprises obtaining said user-specific information from the secure electronic system.

13. (Cancelled)

14. (Original) A method according to claim 1, wherein step c) further comprises storing said process log in a log database.

15-16. (Cancelled)

17. (Original) A method according to claim 1, comprising an additional step before step d) of providing an audit trail of the signing of step b) in the document as signed.

18. (Original) A method according to claim 17, wherein said additional step comprises including a secure document authentication code uniquely representing said document as signed in said audit trail.

19. (Original) A method according to claim 18, wherein said additional step further comprises storing said secure document authentication code in a database.

20. (Original) A method according to claim 18, wherein said additional step further comprises generating a hash of said document as signed defining the secure document authentication code.

21. (Original) A method according to claim 1, comprising an additional step before step d) of embedding a secure document authentication code uniquely representing the document as signed inside said document.

22. (Original) A method according to claim 1, wherein step d) comprises transmitting a copy of the document as signed to the user.

23. (Original) A method according to claim 1, wherein step d) comprises enabling the user to download the document as signed.

24. (Original) A method according to claim 1, wherein step d) further comprises making the document as signed available to at least one additional party concerned by said electronic document.

25. (Currently Amended) A web-based method for applying a legally enforceable signature of a user on an electronic document located on a server, the signing of said document occurring in a web environment, said method comprising the steps of:

a) having the user access the web environment through a web browser from a secure electronic system, said secure system having verified an identity of the user;

b) having the user sign the electronic document in said web environment, said signing ~~being server-based and~~ comprising modules on the server performing the substeps of:

i) presenting the user with legal information related to said signing, and getting agreement from the user of said legal information in said web browser;

ii) presenting the user with a web-based representation of the document information in said web browser;

iii) getting confirmation from the user that the document is to be signed information through said web browser; and

iv) applying said signature of the user on said document on the server;

c) on the server, generating a process log of the signing of step b), said process log comprising a record of ~~allowing the reconstruction of~~ substeps b) i) to b) iv) as executed ~~by said user user~~ and allowing the reconstruction of the web-based representation of the document and of the legal information as presented to the user through said web browser, and securely associating said process log with the document as signed, said securely associating comprising the substeps of:

i) generating a secure process authentication code uniquely representing said process log, said secure process authentication code being a hash of said process log; and

ii) embedding said process authentication code in said document as signed, thereby securely associating said process log and document; and

d) making the document as signed available to the user.

26. (Original) A method according to claim 25, wherein, in step b) i), said legal information comprises information about legal implications of the signing of the document.

27. (Original) A method according to claim 25, wherein, in step b) i), said legal information comprises legal disclosures related to said document.

28. (Original) A method according to claim 25, wherein substep b) i) comprises presenting said legal information in a series of web pages.

29. (Original) A method according to claim 25, wherein substep b) i) comprises presenting said legal information in a series of dialog boxes.

30. (Original) A method according to claim 25, wherein substep b) ii) comprises retrieving said document from a document storing location.

31. (Original) A method according to claim 25, wherein substep b) ii) comprises generating said document from a template.

32. (Original) A method according to claim 25, wherein substep b) ii) comprises transforming said document from a non-web format to a web-format.

33. (Original) A method according to claim 25, wherein substep b) iv) comprises associating user-specific information to said document.

34. (Original) A method according to claim 33, wherein, in substep b) iv), said user-specific information is included in a special signature file defining the signature of the user.

35. (Original) A method according to claim 33, wherein substep b) iv) further comprises associating a digital certificate and private key to the document.

36. (Original) A method according to claim 33, wherein substep b) iv) further comprises obtaining said user-specific information from the secure electronic system.

37. (Cancelled)

38. (Original) A method according to claim 25, wherein step c) further comprises storing said process log in a log database.

39-40. (Cancelled)

41. (Original) A method according to claim 25, comprising an additional step before step d) of providing an audit trail of the signing of step b) in the document as signed.

42. (Original) A method according to claim 41, wherein said additional step comprises including a secure document authentication code uniquely representing said document as signed in said audit trail.

43. (Original) A method according to claim 42, wherein said additional step further comprises storing said secure document authentication code in a database.

44. (Original) A method according to claim 42, wherein said additional step further comprises generating a hash of said document as signed defining the secure document authentication code.

45. (Original) A method according to claim 25, comprising an additional step before step d) of embedding a secure document authentication code uniquely representing the document as signed inside said document.

46. (Original) A method according to claim 25, wherein step d) comprises transmitting a copy of the document as signed to the user.

47. (Original) A method according to claim 25, wherein step d) comprises enabling the user to download the document as signed.

48. (Original) A method according to claim 25, wherein step d) further comprises sending a copy of the document as signed to at least one additional party concerned by said electronic document.

49. (Currently Amended) A system for applying a legally-enforceable signature of a user on an electronic document in a web environment, the electronic document located on a server, said system comprising:

accessing means for accessing said web environment from a secure electronic system through a web browser;

a document-rendering module on the server for presenting the user with a web-based representation of said document in said web browser;

a legal disclosure module on the server for presenting the user, in said web browser ~~environment~~, with legal information related to electronically signing said document, and for obtaining agreement from the user of said legal information document in said web browser;

a document approval module on the server for providing the signature of the user to the document upon agreement from the user of the legal information, thereby signing said document;

a process log module on the server for generating a process log of the signing of the document and securely associating said process log with the document as signed, said process log comprising reconstruction data for allowing the reconstruction of the presenting the user with said web-based representation of the document, of said presenting the user with said legal information, of said obtaining agreement from the user of said legal information and of said signing of the document, said process log module comprising means for generating a secure process authentication code uniquely representing said process log, and embedding said secure process authentication code in said document as signed, thereby securely associating said process

log and ~~said~~ document, wherein said means to generate a secure process authentication code comprise a hash module; and

a document distribution module for making the document as signed available to the user,

wherein said accessing means and said document-rendering, legal disclosure, document approval, process log and document distribution modules are server-based.

50. (Original) A system according to claim 49, wherein said document-rendering module comprises retrieving means for retrieving said document from a document storing location.

51. (Original) A system according to claim 49, further comprising a document customization module cooperating with the document-rendering module for generating said document from a template.

52. (Original) A system according to claim 49, wherein said document-rendering module comprises transforming means for transforming said document from a non-web format to a web-format.

53. (Original) A system according to claim 49, wherein said legal information comprises information about legal implications of the signing of the document.

54. (Original) A system according to claim 49, wherein said legal information comprises legal disclosures related to said document.

55. (Original) A system according to claim 49, wherein said legal disclosure module comprises displaying means for displaying said legal information in a web-based medium.

56. (Original) A system according to claim 55, wherein said web-based medium includes a plurality of web pages.

57. (Original) A system according to claim 55, wherein said web-based medium includes a plurality of dialogue boxes.

58. (Original) A system according to claim 49, further comprising a user binding module cooperating with the secure electronic system to obtain therefrom user-specific information, generating a special signature file using said user-specific information and providing said special signature file to the document approval module, said special signature file defining the signature of the user.

59. (Original) A system according to claim 58, wherein said user-specific information comprises a digital certificate and private key.

60-62. (Cancelled)

63. (Original) A system according to claim 49, further comprising an audit trail module for providing an audit trail of the signing of the document in said document as signed.

64. (Original) A system according to claim 63, wherein said audit trail includes a secure document authentication code uniquely representing said document as signed.

65. (Original) A system according to claim 64, wherein the document authentication code is a hash of said document as signed.

66. (Original) A system according to claim 49, wherein the document approval module comprises means for embedding a document authentication code uniquely representing the document as signed inside said document.

67. (Original) A system according to claim 49, wherein said document distribution module comprises means for transmitting a copy of the document as signed to the user.

68. (Original) A system according to claim 69, wherein said document distribution module provides a copy of the document as signed to at least one additional party concerned by said electronic document.